425 Forensics Report

# Searching for ASCII strings

The ASCII string search function can be found via the command **search** from the program's main screen. The program will prompt the user for a target directory, followed by multiple keywords. The inputs should be entered in the following format:

Directory: /*home/cosc/student/jam296/Desktop*  
Keyword: *keyword otherkeyword*

The keywords will be converted to lowercase to maximise search results.

The directory is traversed via a depth-first in order method. Any file names containing the keywords are added to a results list (a vector) containing the path to the file. If the title does not contain a keyword, the file is then read line-by-line into a buffer, which is converted to lowercase and searched for the keywords. If a keyword is found within the file, the file's path is also added to the results list. Only Directories and Regular files are searched - other file types such as pipes are not searched as it would cause the program to hang.

When the directory traversal is complete the results list is displayed in a numbered order. From this state the user can enter the following commands:

open #: This will open the file with the program assigned to handling this file's type.  
hexedit #: This will pass the file through to the program's hex editor. See Hexadecimal Editor for more.  
back: returns the user to the main screen.

Multiple files can be opened and edited without having to re-search. The results are held until the user returns to the main menu.

# Searching for Hexadecimal strings

The Hexadecimal search function can be accessed via the command **hexfind** from the program's main screen. This program prompts the user for a directory and a hex string to search for. Unlike the search function, the hexadecimal value is not converted to lowercase. Hexadecimal values are interpreted case-sensitively, and the string input should consist of uppercase characters. For example:

Correct: 46757A7A [will search for "Fuzz"]  
Correct: 66757A7A [will search for "fuzz"]  
Incorrect: 66757a7a [all characters in the input should be uppercase]

Search methods here are similar to the ASCII string search function, with the notable exception of file parsing; the lines are not converted to lowercase, they are converted to hex and then searched.

The search results are displayed in the same way as ASCII results, and the same operations can be performed on them.

# C:\Users\Joel\Desktop\Downloads\Screenshot at 2012-04-25 22_36_14.pngHexadecimal editor

The Hexadecimal editor can be accessed from both the main menu via the command **hexedit**, or calling it from within the search results function.

Accessing it from the main menu prompts the user for a file path, which should be entered without quotes as follows:

*/home/cosc/student/jam296/Desktop/findme.txt*

To access it from the search results, the user should type "hexedit **#**" where **#** is the listed number of the file they wish to edit.

From the main screen of the hex editor the user can type:

display: Displays the contents of the file in hexadecimal  
replace [**pos**] [**val**]: replace the value at position **pos** with value **val**back: returns the user to the previous screen - either the search results screen or the main screen.

search | hexfind

replace [pos] [val]

open #

hexedit #

path

dir

keyword

Enter Directory

back

Convert to Lowercase

Convert to Hexadecimal

Output Results

display

Replace Function

hexedit

Traverse & Search

Hex Editor

Display

Open File

Enter File Path

Enter Hex String

Enter Keyword

Traverse & Search

Main Interface